

**i Exam information****University of Oslo - Faculty of Mathematics and Natural Sciences****Digital exam in INF3510 Information Security (Spring 2018)****Date and time:** 1 June 2018, 09:00h - 13:00h**Permitted materials:** Language dictionary

Please regard the following directions:

- The exam contains 44 questions with a total of 100 points (= 100 %).
- Each question states explicitly the marking scheme.
- Some parts of a question may give negative marks when answered incorrect, but the total score for each question is always at least 0 points (never negative).
- The questions are grouped under 10 parts that correspond approximately to 10 of the lectures in this course.
- Be concise. When answering a question, it is often sufficient to write a single expression or sentence to describe each concept that the question asks for.
- Answers can be written in English or in Norwegian.

**i Part 1: General Security****1 ISO27000**Write the definition (approximately) of *information security* according to ISO27000.*Points: max 2 total score***Fill in your answer here**

Preservation of confidentiality, integrity and availability of information

Maximum marks: 2

**2 Availability I**Write the definition (approximately) of *availability* according to ISO27000.*Points: max 1***Fill in your answer here**

The property of being accessible and useable upon demand by an authorized entity

Maximum marks: 1

### 3 Availability II

Which is the most relevant *threat* against availability?

Points: 1 for correct answer, 0 for wrong or no answer

Select one alternative:

- DDoS attack
- Phishing email
- Cryptanalysis
- Zero-day exploit
- SQL injection



Maximum marks: 1

### 4 Authentication

Select the two (2) *most general* categories of authentication.

Points: 1 for each correct, 0 for each wrong, 0 for no answer, max 2 total score

Select two alternatives:

- Entity authentication
- Server authentication
- Data authentication
- User authentication
- Knowledge-based authentication
- Token-based authentication



Maximum marks: 2

### 5 Authorization

Explain the concept of *authorization* in a way consistent with the definition of confidentiality.

Points: max 1

Fill in your answer here

The process of defining the access control policy, i.e. who is authorized to access a resource

Maximum marks: 1

### 6 Data Origin

Indicate whether each characteristic in the left column is relevant for *non-repudiation* or *authentication of data origin*. Some characteristics are irrelevant, in that case select 'irrelevant'.

Points: 0.5 for each correct relevance, -0.5 for each wrong, 0 for no marking in a row, max 3

Select the correct relevance:

	Non-repudiation	Authentication	Irrelevant
Implemented with digital signature	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Implemented with MAC	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Proof to both recipient and to any 3rd party	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Proof only to recipient	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Always multi-factor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
Always based on biometrics	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>

Maximum marks: 3

## i Part 2: Cryptography

### 7 Hash Functions I

Select the properties of (good) hash functions.

Points: 1 for each correct, 0 for each wrong, 0 for now answer, max 2 total score

Select one or more alternatives:

- Assymmetric
- Confidential
- Bijective
- One way ✓
- Collision resistance ✓

Maximum marks: 2

### 8 Hash Functions II

Name two (2) common applications of cryptographic hash functions.

Points: max 2

Fill in your answer here

HMAC, Digital Signature, Password Storage, Challenge Response Protocols

Maximum marks: 2

## 9 MAC

What is the purpose of sending a message with a MAC?

Points: 1 for correct answer, 0 for wrong answer

Select one alternative:

- The recipient can authenticate the message origin. ✓
- It provides non-repudiation of message origin.
- It protects the message confidentiality.
- Any third party can authenticate the message origin.

Maximum marks: 1

## 10 Symmetric Encryption

Specify the possible *key sizes* (in bits) of the AES encryption algorithm.

Points: 1 for each correct, 0 for each wrong, max 2 total score

Smallest block size:  (128)

Largest block size:  (256)

Maximum marks: 2

## 11 Asymmetric Encryption

Alice wants to send a message to Bob, encrypted with RSA. Which key does she use for the encryption process?

Points: 1 for correct answer, 0 for wrong answer

Select an alternative:

- Alice's public key
- Alice's private key
- Bob's private key
- Bob's public key ✓

Maximum marks: 1

## 12 Quantum Computing

What will be the influence of quantum computing on current crypto systems?

Points: 1 for each correct, 0 for each wrong, max 2 total score

Select one or more alternatives:

- Symmetric crypto algorithms (e.g. AES) will be completely broken.
- Asymmetric crypto algorithms (e.g. RSA) will need larger keys.
- There will be no effect.
- Symmetric crypto algorithms (e.g. AES) will need shorter keys.
- Symmetric crypto algorithms (e.g. AES) will need larger keys. ✓
- Asymmetric crypto algorithms (e.g. RSA) will be completely broken. ✓

Maximum marks: 2

## i Part 3: Key Management

### 13 Key distribution

Select for each key type the correct statement that applies for **key distribution** of the specific key type.

Points: 1 for each correct, -1 for wrong, 0 for no answer, max 3 total score

Select the correct statement.

	Keys are not distributed	Authenticity required	Confidentiality required	None of the other statements
Symmetric keys	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Asymmetric private keys	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Asymmetric public keys	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maximum marks: 3

### 14 Certificates

Please mark the three (3) most relevant elements inside a X.509 certificate.

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 3 total score

**Select one or more alternatives:**

- Public key of the subject ✓
- Key exchange algorithm
- Common name of the subject ✓
- Signature created by the issuer ✓
- Public key of the issuer
- Signature created by the subject
- IP Address of the issuer

---

Maximum marks: 3

## 15 PKI

Please mark the statements on **certificates** and **browser PKIs** (Public Key Infrastructure) which are true.

*Points: 1 for each correct, 0 for wrong, 0 for no selection, max 2*

**Select one or more alternatives:**

- Certificates ensure authentic exchange of private keys.
- Certificate Transparency allows automatic issuing of certificates.
- A CA verifies the ownership of a domain before signing the certificate. ✓
- Certificates allow the user to detect phishing Web sites.
- For an extended validation certificate (EV), the requester must proof the honest intention of the Web site.
- The trust model is based not on one, but on many root CAs. ✓

---

Maximum marks: 2

## 16 Certificate Revocation

Please name two (2) common methods for **certificate revocation**.

*Points: max 2*

**Fill in your answer here**

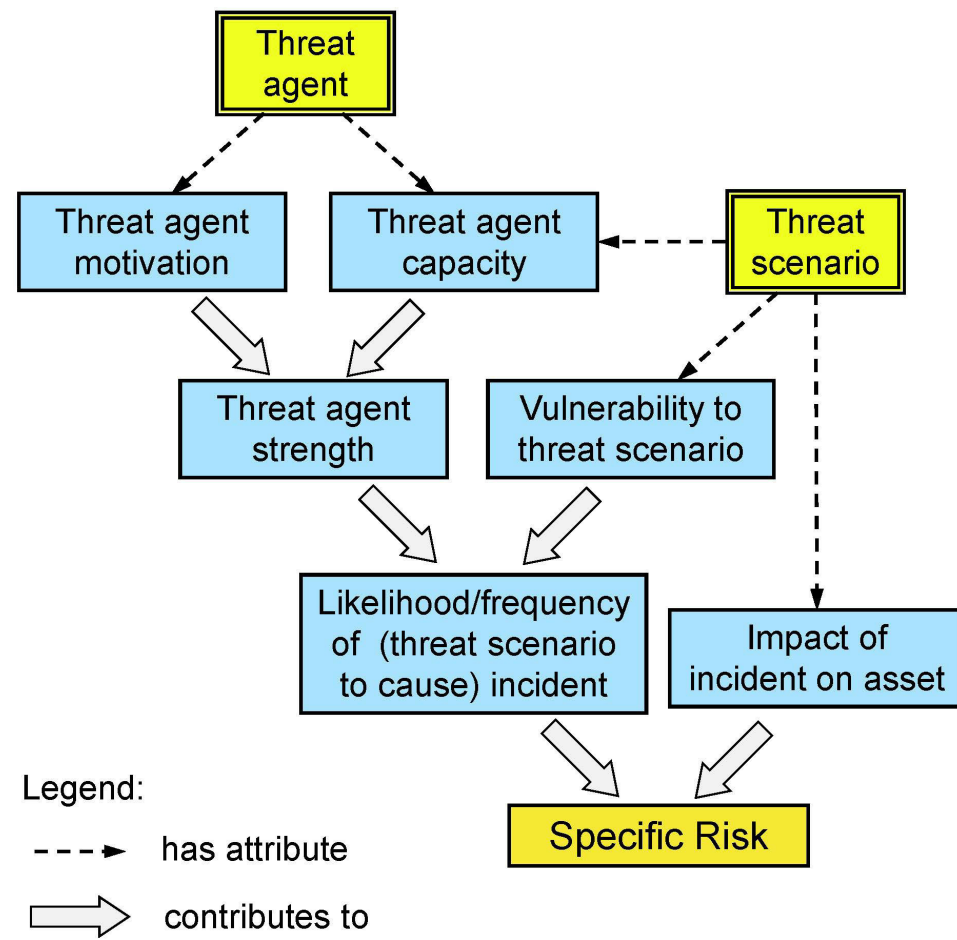
CRL, OCSP

---

Maximum marks: 2

## i Part 4: Risk Management

## 17 Practical Risk Model



Select two elements from the diagram that must be specified in a typical practical method for qualitative assessment of risks.

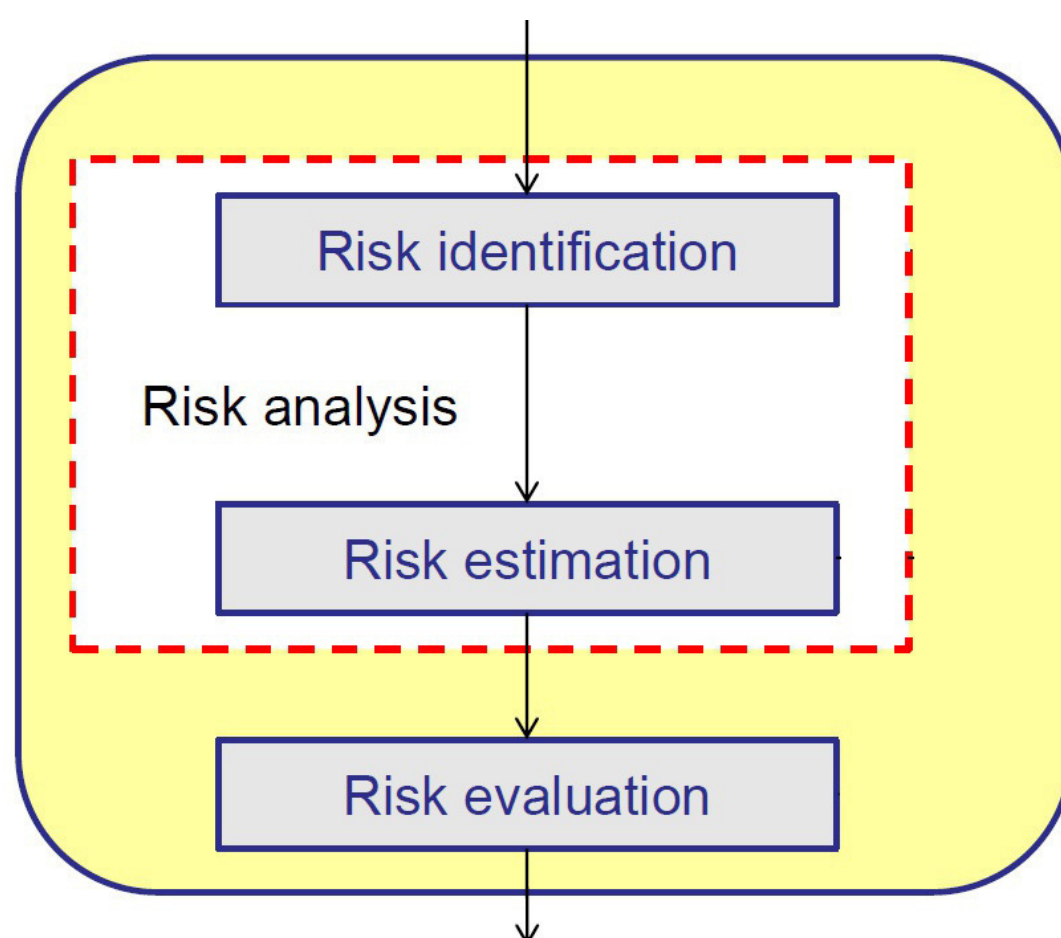
Points: 1 for each correct selection, 0 for each wrong, 0 for no selection, max 2 total score

Select two alternatives:

- Impact on assets ✓
- Threat agent motivation
- Likelihood of incident ✓
- Vulnerability to threat scenario
- Threat agent strength
- Threat agent capacity

Maximum marks: 2

18 Risk Assessment



Risk Identification and Risk Estimation are different steps as part of risk assessment in the risk management



process.

Mention two (2) elements of *Risk Identification* and two (2) elements of *Risk Estimation*.

Points: 1 for each correct element, max 4 total score

#### Risk Identification

Identification of: assets, threats, existing controls, vulnerabilities, consequences

#### Risk Estimation

Assess asset values and impacts; Assess incident likelihood/frequency; Determine/compute risk levels

Maximum marks: 4

## 19 Threat modelling

Select two (2) relevant approaches for identifying/modelling threat scenarios.

Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score

Select two alternatives:

- Asset-centric threat modelling ✓
- Vulnerability-centric threat modelling
- Impact-centric threat modelling
- Attacker-centric threat modelling ✓

Maximum marks: 2

## 20 Risk Levels

Please mention for qualitative and quantitative risk analysis one example each.

Points: 1 for each correct answer, max 2 total score

#### Qualitative

- Impact level: Minor, moderate, major, catastrophic
- Likelihood: Rare, unlikely, possible, likely, almost certain

#### Quantitative

- Consequence (e.g. \$\$\$)
- Likelihood (e.g. probability value)

Maximum marks: 2

## i Part 5: Computer Security



## 21 Protection Rings

Assign the protection rings to the modes.

Points: 0.5 for each correct, -0.5 for wrong, 0 for no answer, max 3 total score

Please match the values:

	Kernel Mode	User Mode	Hypervisor mode	Not used (anymore)	Does not exist
-1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
0	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓

Maximum marks: 3

## 22 Virtualization

Select the statements on platform virtualization which are true.

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score

Select one or more alternatives:

- A guest OS can access another guest OS, which is located on the same host system.
- Platform virtualization increases the energy demand.
- The hypervisor is always running on top of the host OS.
- The hypervisor offers virtual hardware interfaces to the VMs. ✓
- Guest VMs on the same host system must have the same OS.
- Platform virtualization helps in malware protection. ✓

Maximum marks: 2

## 23 Trusted Computing

Explain (shortly!) the motivation/idea of trusted computing.

Points: max 2

Fill in your answer here

Software alone can not be trusted. Use specialised security hardware in a computer system.

**24 TPM**

TPM (Trusted Platform Module) is a hardware chip which supports three (3) main security services on computing platforms. List these three main *TPM-supported services*:

*Points: max 3 total score*

**Fill in your answer here**

- Authenticated/measured boot,
- Sealed Storage / Encryption
- Remote attestation

Maximum marks: 3

**i Part 6: User Authentication****25 Authentication Factors**

Name the three (3) general credential categories (called *authentication factors*)

*Points: 0.5 for each correct answer, 0 for wrong, 0 for no answer*

Knowledge, Ownership, Inherence (Biometrics)

Give an example for an existing wide-spread 2-factor authentication system.

*Points: 0.5 for correct answer, 0 for wrong, 0 for no answer*

ATM (card + PIN), Google (password + phone), ...

Maximum marks: 2

**26 Password Storage**

Select the relevant *security method* for implementing each requirement in password databases.

*Points: 0.5 for each correct, -0.5 for wrong, 0 for no answer, max 2 total score*

Select the relevant security method:

	Access Control	Complex password	Salting	Hashing
Only authorized entities can read the password database	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Passwords are not readable in the database	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Pre-computed hash tables can not be used to crack passwords	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Attackers can not crack a salted and hashed password in the database	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>

Maximum marks: 2

## 27 Biometrics

Name one (1) advantage and two (2) disadvantages/problems/challenges of *biometric authentication*.

Points: 1 for each correct answer, 0 for wrong answer, 0 for no answer, max 3 total score.

**Advantage**

Easy to use, can not loose/forget authorization credentials, ...

**Disadvantages/Problems/Challenges**

High false negative rate, low performance, threat for personal safety (e.g. cut finger), threat for privacy (e.g. reveal illness), usability (e.g. handicapped persons)

Maximum marks: 3

## 28 Authentication Tokens

Mention and briefly describe the two (2) types of *synchronised authentication tokens*.

Points: 1 for each correct, 0 for no answer, 0 for wrong answer, max 2 total score

**Fill in your answer here**

clock-based: client and server have (synchronized) internal clocks, that are used to derive an OTP  
 counter-based: client and server have a counter, which is used to derive an OTP. After each authentication action, the counter is incremented

Maximum marks: 2

## 29 Authentication Assurance Level

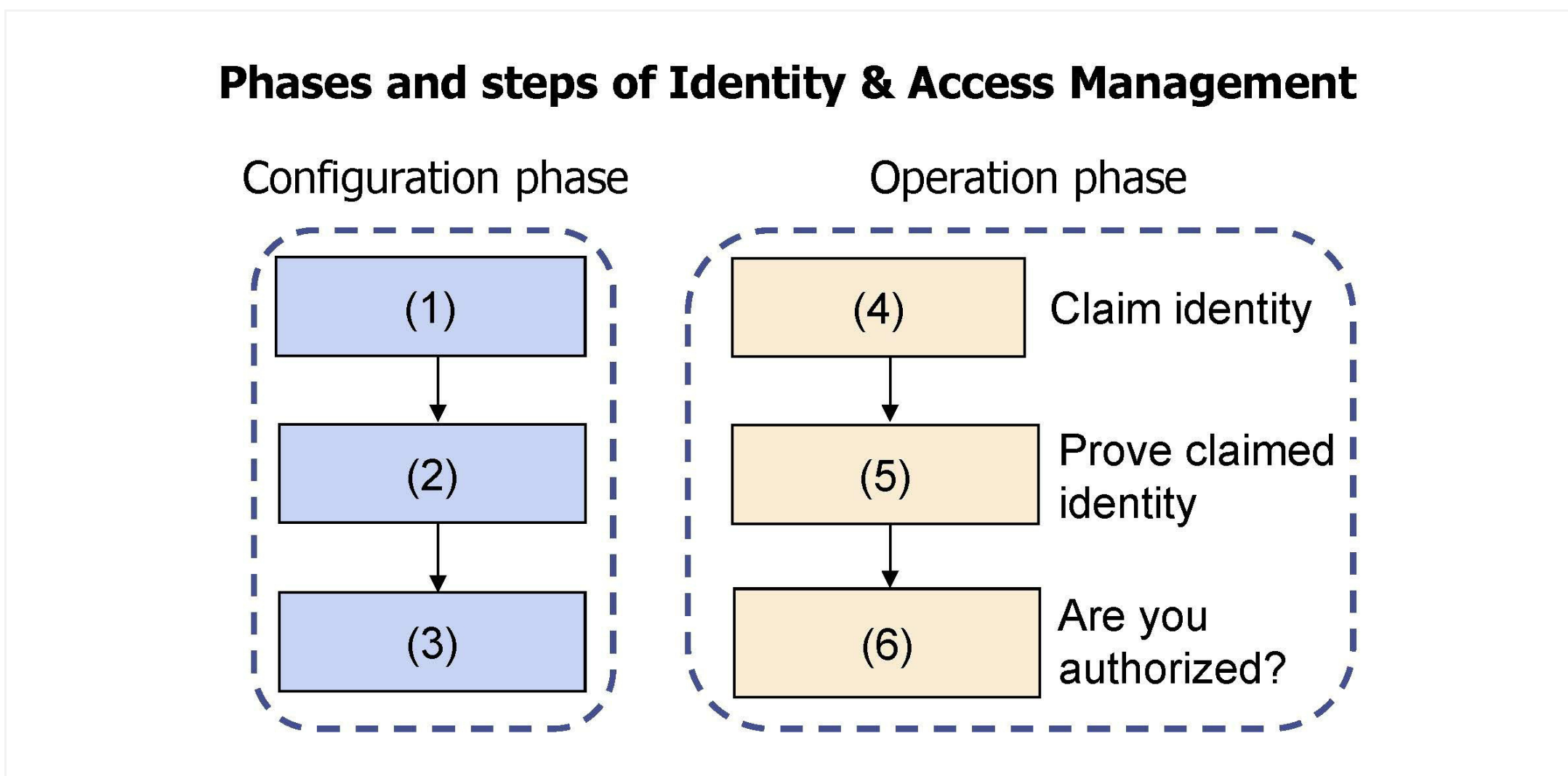
How many AALs (Authentication Assurance Levels) do the European eIDAS framework specify ?  (3).

Points: 1 for correct, 0 for wrong, 0 for no answer

Maximum marks: 1

**i Part 7: Identity & Access Management**

**30 Phases in Identity & Access Management**



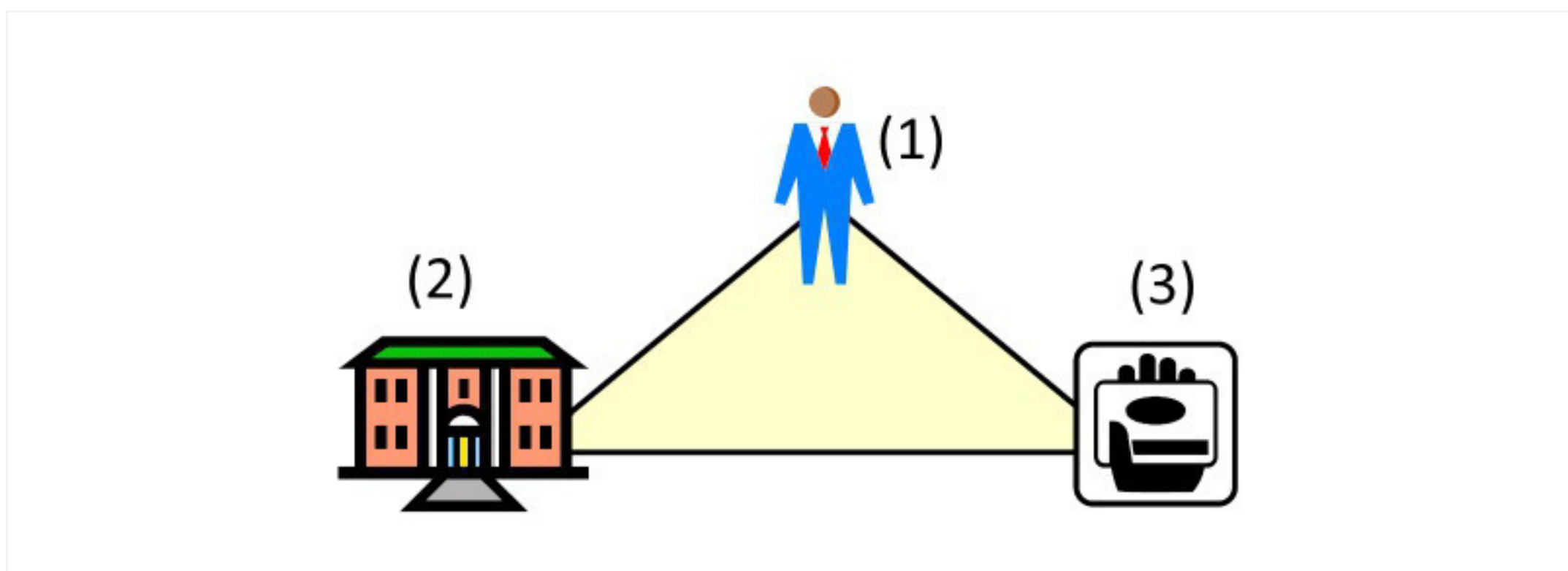
The diagram shows that the configuration phase and the operation phase of IAM (Identity & Access Management) consists of steps which represent specific activities. Match each activity in the left column with the corresponding step in the diagram.

Points: 0.5 for each correct, -0.5 for each wrong, 0 for no selection, max 3

**Match activity with step number:**

	1	2	3	4	5	6
Access Control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Authorization	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Self Identification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provisioning	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Registration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maximum marks: 3

31 **Federation I**

Name the three components in a standard *federation* environment.

Points: 1 for each correct answer, 0 for wrong, 0 for no answer, max 3 total score

(1)

User

(2)

Service Provider (SP)

(3)

Identity Provider (IdP) or Credential Provider (CrP)

Maximum marks: 3

32 **Federation II**

Select the *federation type* of the eduroam system.

Points: 1 for correct, 0 for wrong, 0 for unanswered

Select an alternative:

- Centralized Identity + Distributed Authentication
- Centralized Identity + Centralized Authentication
- Distributed Identity + Centralized Authentication
- Distributed Identity + Distributed Authentication



Maximum marks: 1

33 **Access Control**

Select the correct statements on *access control* (DAC = Discretionary Access Control, MAC = Mandatory Access Control, RBAC = Role-Based Access Control, ACL = Access Control List)

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 3 total score

**Select one or more alternatives:**

- In MAC the user defines the access to the resource he has created.
- MAC is typically implemented with ACLs
- DAC is used in Linux systems. ✓
- An ACL maps a user to role.
- RBAC can be combined with DAC. ✓
- In RBAC, users can own multiple roles. ✓

---

Maximum marks: 3

**i Part 8: Communication Security****34 Security Protocols**

Specify the respective OSI layers TLS and IPSec are operating on.

*Points: 1 for each correct, 0 for wrong, 0 for no answer.*

TLS:  (4), IPSec:  (3)

---

Maximum marks: 2

**35 TLS I**

Select for the following statements if they are true or false.

*Points: 0.5 for each correct, -0.5 for each wrong, 0 for no answer, max 4 total score*

Please match the values:

	false	true
If activated, TLS secures all TCP connections originated from that computer.	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
For exchange of session keys, RSA is more secure than DH.	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
HTTP and HTTPS can be offered on the same TCP port.	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
TLS ensures integrity of transferred data.	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
Client and server must authenticate inside a TLS connection.	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
The algorithms used inside a session are negotiated between client and server.	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
The session key is created during the TLS handshake from 3 random numbers.	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
The subject of the server certificate must be equal to the server's host name entered in the browser.	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>

Maximum marks: 4

36 **TLS II**

Name two (2) weaknesses/attacks for TLS.

*Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score***Fill in your answer here**

Attacks: SSL Striping, BEAST, POODLE, DROWN, ROBOT, FREAK, Logjam, ...  
 Outdated algorithms (MD5, 3DES, RC4, ...)  
 Attacks on certificates/PKI, TLS inspection

Maximum marks: 2

37 **TOR**

Explain the metaphor "onion" in the TOR system.

*Points: max 2 total score*



Fill in your answer here

The message is first encrypted for the final router, the result for the 2nd last router, the result for the 3rd last router, ...  
This forms multiple "skins" like at an onion.

Maximum marks: 2

## i Part 9: Network Perimeter Security

### 38 Firewall

Select the statements on firewalls which are true:

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score

Select one or more alternatives:

- A network firewall is named like this, because it completely separates two networks.
- The Linux iptables is an implementation of an application layer proxy.
- Stateful packet filters can correlate a DNS response to a prior DNS request. ✓
- In proxy mode, the client makes a TCP connection to the firewall and the firewall creates a second TCP connection to the server. ✓
- A packet filter operates on network layer 3 and 2.
- A application layer proxy can handle all protocols on top of TCP.

Maximum marks: 2

### 39 TLS Inspection

Briefly explain how a user can know whether the TLS-encrypted traffic from a workstation in a company to a remote server on the Internet is being inspected in the company gateway firewall.

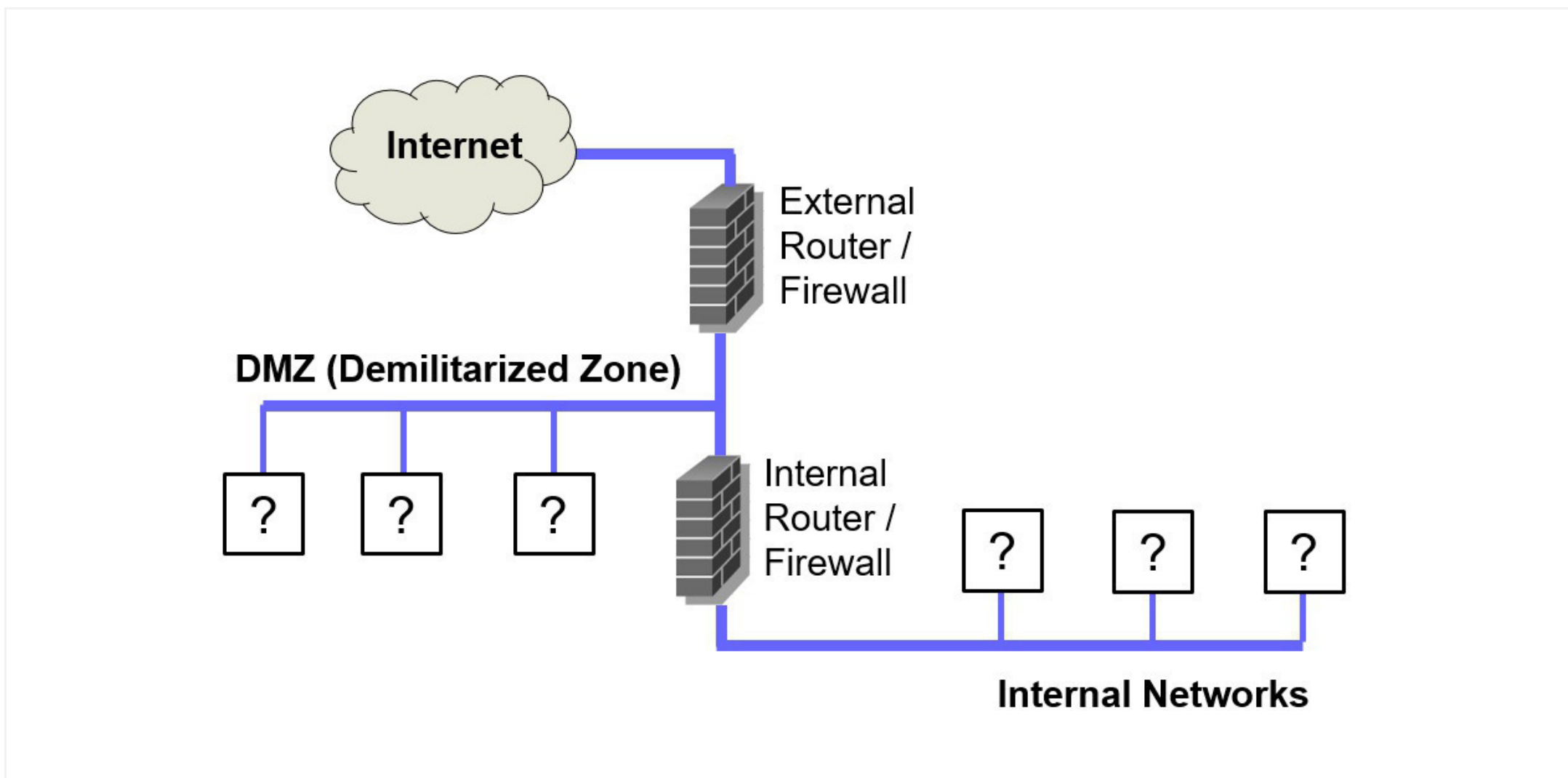
Points: max 2 total score

Fill in your answer here

All certificates in TLS connections are issued by the same CA - the one build inside the TLS gateway.  
(Additionally: the certificate root store contains the certificate of the TLS gateway)

Maximum marks: 2

### 40 DMZ



In the case of two firewalls with a so-called DMZ (Demilitarized Zone) between them, servers/systems can be connected to either the DMZ or to internal networks. Select the typical location for connecting the servers/systems in the left column below.

Points: 0.5 for each correct, -0.5 for wrong, 0 for unanswered, max 3 total score

Select correct placement of each type of system:

	DMZ	Internal Networks
Database Server	<input type="radio"/>	<input type="radio"/> ✓
DNS Server	<input type="radio"/> ✓	<input type="radio"/>
Email server	<input type="radio"/> ✓	<input type="radio"/>
Production Server	<input type="radio"/>	<input type="radio"/> ✓
Web Server	<input type="radio"/> ✓	<input type="radio"/>
Workstation	<input type="radio"/>	<input type="radio"/> ✓

Maximum marks: 3

41 **IDS**

The two main techniques used in IDS (Intrusion Detection Systems) are Signature-Based Detection and Anomaly-Based Detection respectively. Select the *relevant IDS technique* for each property in the left column below.

Points: 0.5 for each correct, -0.5 for wrong, 0 for unanswered, max 3 total score

Select the relevant IDS technique for each property:

	Anomaly Detection	Signature Detection
Generates relatively many false intrusion alarms	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Generates relatively few false intrusion alarms	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
Can detect unknown attacks	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Based on known attacks	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>
Based on learning normal behaviour	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Can only detect known attacks	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>

Maximum marks: 3

**i Part 10: Application Security**

**42 Malware**

Select the relevant type of malware according to each description in the left column below.

Points: 1 for each correct, -1 for wrong, 0 for no answer, max 4 total score

Select the relevant type of malware:

	Exploit	Worm	Trojan	Virus
A user-installed program with hidden malicious functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>
Malicious software or data that exploits a software/hardware vulnerability in systems	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A self-replicating independent malicious program	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
Self-replicating malicious code which is injected into other programs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="checkbox"/>

Maximum marks: 4

**43 OWASP**

Mention the meaning of the acronym *OWASP*, and briefly describe what the '*OWASP Top 10*' is.

Points: max 2 total score)

**Fill in your answer here**

- Open Web Application Security Project
- The most widespread Web Application weaknesses

Maximum marks: 2

**44 SQL Injection**

Assume a Web login, where the user can enter an email address and a password. The entered parameters (<*email*> and <*passwd*>) are forwarded to the following SQL statement inside the Web application:

```
SELECT userid FROM user WHERE email = '<email>' AND passwd = '<passwd>';
```

If the SQL result is ~~none~~<sup>not</sup> empty, the user is authenticated.

An attacker enters as password:

```
x' or '1' = '1
```

What will happen?

Points: max 2

**Fill in your answer here**

With the entered "password" the WHERE clause is evaluated to TRUE and the SELECT statement returns the complete userid table. Thus, the application assumes a correct password was entered and the attacker is authenticated as the user with the given email address.

What countermeasures can be applied to fix the previous problem?

Points: max 2

**Fill in your answer here**

Sanitize data input  
Use prepared SQL statements

Maximum marks: 4